To: Los Angeles From: Milwaukee
Re: [redacted] 03/20/2001

b3
b7E

LEAD(s):

Set Lead 1:

LOS ANGELES

AT IRVINE, CA

Contact the University of California, Irvine. Determine if the server, IP address 128.200.9.133, domain name franco.eng.uci.edu, was a victim of an intrusion on or about January 14, 2000. If so, conduct a logical investigation of the incident. Report to Milwaukee Division of the damages associated with this possible intrusion, and subsequent DOS attack.

♦♦

(Rev. 08-28-2000)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/20/2001

To: Los Angeles **Attn:** NIPC Squad
SA [redacted] b6 b7C

From: Milwaukee
Squad 5
Contact: SA [redacted] Ext. (414) 291-4837

[redacted] **oved By:** [redacted] b3 b6 b7C b7E

Drafted By:

Case ID #: [redacted] (~~Pending~~) [redacted]

Title: [redacted] ET. AL.;
INFINITY TECHNOLOGIES, INC., ET. AL.;
UNAUTHORIZED ACCESS, ET. AL.;
NIPCIP

Synopsis: The purpose of this communication is to set forth lead for Los Angeles Division.

Details: For the information of the Los Angeles Division, Milwaukee Division is investigating various criminal activities conducted by the captioned subject, [redacted] also known as [redacted] and his associates, also known as the REALM OF CHAOS. These criminal activities included computer related acts such as unauthorized intrusions and software piracy. Other criminal acts included manufacturing explosives, and over one hundred acts of malicious destruction directed at energy facilities, telecommunication facilities, and government facilities. b6 X b7C [redacted]

Among the criminal computer activities conducted by [redacted] it is believed that one of seven denial of service (DOS) attacks perpetrated against one of [redacted] victims, Ultimate Fun World Two (UF2) originated from a University of California, Irvine, server, domain name "franco.eng.uci.edu", Internet protocol (IP) address 128.200.9.133. The technical documentation provided by UF2 indicated that [redacted] OAC-DCS, at UC Irvine, was familiar with the situation, and had worked with Norlight Telecommunications, UF2's upstream Internet access provider, to resolve the DOS attack on the UF2. The victim IP address at UF2 was 209.83.44.145, which was the UF2 domain name services (DNS) server. This attack occurred on January 14, 2000. b6 b7C

[redacted] b3 b6 b7C b7E